Les algorithmes cryptographiques

Guillaume Lelaurain

journées Chiffrement

CNRS / UREC

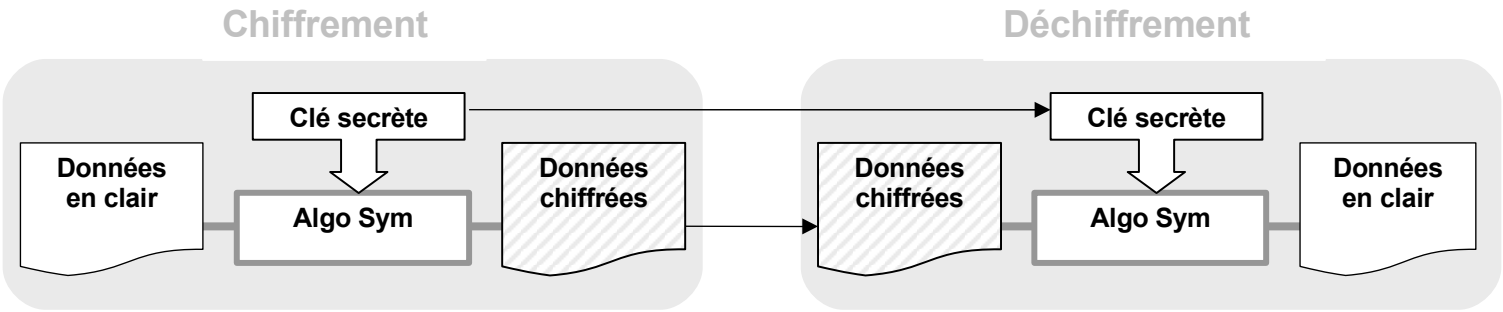
Le 24 janvier 2006

Les algorithmes cryptographiques – Plan

- Les types de chiffrement
  - Symétrique, Asymétrique, Hybride
- Les principaux algorithmes rencontrés
  - DES & 3DES, AES, Blowfish et finalistes AES
  - RSA
- D'autres mécanismes utilisés
  - Hachages, HMAC, signatures
- Recommandations
  - Algorithmes et longueurs de clés

Type de chiffrement - Symétrique

- Principe



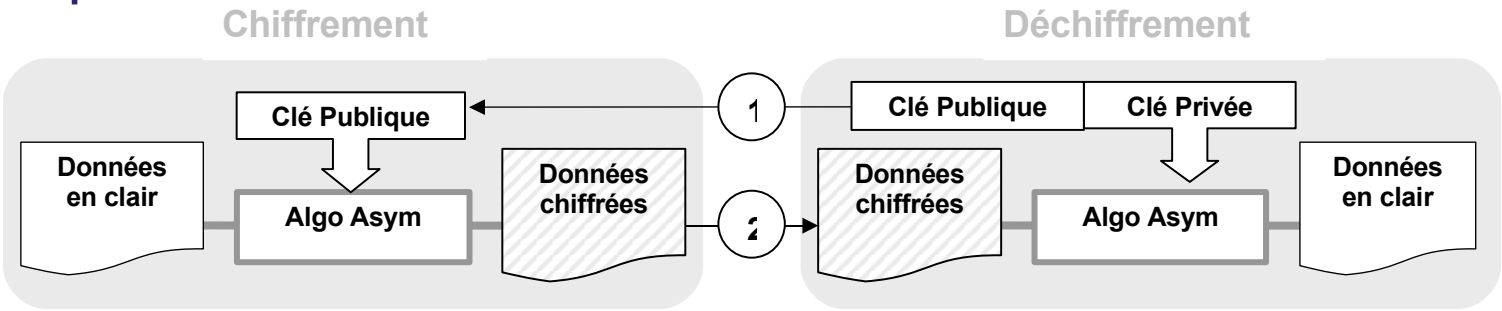
- Mode de fonctionnement
  - Par flux : ECB (Electronic CodeBook)
  - Par chaînage de blocs : CBC (Cipher Block Chaining)

- Caractéristiques principales
  - Clé unique pour le chiffrement et le déchiffrement
  - Rapide
  - Nécessite un échange sécurisé de la clé

Type de chiffrement - Asymétrique

Concept publié par Diffie, Hellman et Merkle en 1975

- Principe

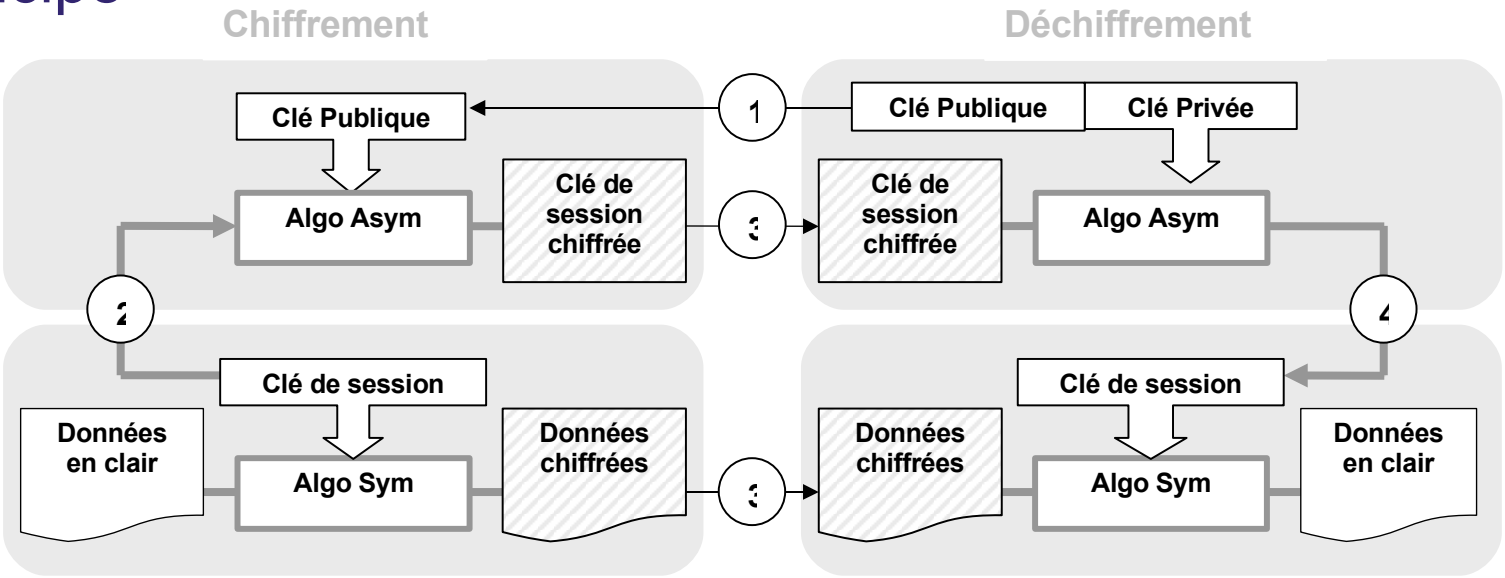


- Caractéristiques principales
  - Deux clés pour le chiffrement et le déchiffrement
  - Lent
  - Elimine le problème de diffusion d'une clé secrète
  - Pose le problème de certification de la clé publique
  - Permet la signature (non-répudiation)

Type de chiffrement - Hybride

Concept mis en œuvre par Zimmermann pour PGP en 1991

- Principe



- Caractéristiques principales
  - Utilise la rapidité de l'algorithme symétrique, et la sécurité de l'asymétrique
  - Utilisé dans la plupart des outils actuels

Algorithme symétrique – DES et 3DES

DES : Tiré de l'algorithme « Lucifer » imaginé par Feistel (IBM)
Adopté comme premier standard en 1977 sous le nom « Data Encryption Standard »

3DES : Même algorithme que DES mais l'opération est répétée 3 fois.

- Caractéristiques principales
  - DES : Clés de 56 bits sur blocs de 64 bits
  - 3DES : Clés de 128-192 ou 112-168 bits sur blocs de 64 bits
  - En fin de vie

- Références
  - http://csrc.nist.gov/publications/fips/fips46-3/fips46-3.pdf

Algorithme symétrique – AES

Algorithme « Rijndael » conçu par deux chercheurs Belges Joan Daemen et Vincent Rijmen

Face à l'obsolescence de DES le NIST organise un appel d'offre pour adopter un nouveau standard. Cinq algorithmes seront reconnus fiables et Rijndael sera adopté comme nouveau standard en 2000 sous le nom « Advanced Encryption Standard »

- Caractéristiques principales
  - Clés de 128, 192, 256 bits sur blocs de 128, 192 ou 256 bits
  - Libre d'utilisation (standard)
- Références
  - http://csrc.nist.gov/encryption/aes/

Algorithmes symétriques – RC5, Blowfish…

- Blowfich Conçu par Bruce Schneier en 1993
  http://www.schneier.com/blowfish.html
  - Cles de 32 à 448 bits sur blocs de 64 bits
  - Du domaine publique

- RC5, RC6 (Rivest's Code) Conçus par Ronald Rivest pour RSA Security
  - Clés et blocs de longueurs variables
  - Implémentation simple
  - Propriété de la société RSA Security
  - RC6 est finaliste au concours AES

- Towfich, Serpent, Mars
  - Finalistes au concours AES
  - Rapide comparatif : http://www.rsasecurity.com/rsalabs/node.asp?id=2236

Algorithme asymétrique – RSA

Algorithme imaginé par Rivest, Shamir et Adleman (mathématiciens du MIT) en 1977

Fondé sur la difficulté (actuelle) de factoriser des grands nombres. La multiplication de deux grands nombres premiers est considérée comme une fonction à sens unique.

- Caractéristiques principales
  - Longueur de clés variables 1024, 2048 bits
  - Aussi utilisé pour la signature

- Référence :
  - http://www.rsasecurity.com/rsalabs/node.asp?id=2214

Autres algorithmes utilisés

- Les fonctions de hachages

  Génération d'empreintes
  Pour le contrôle d'intégrité des données

  - MD5 produit une empreinte de 128 bits
  - SHA-1 produit une empreinte de 160 bits (existe SHA-224-256-384-512)
  - RIPEMD produit une empreinte de 160 bits

- Code d'authentification de message (Message Authentication Code)

  Empreinte générée avec un secret
  Pour le contrôle d'intégrité et d'origine des données

  - HMAC-MD5 HMAC-SHA1
  - CBC-MAC-X9.19 CBC-MAC-EMAC

- Signatures

  Empreinte d'un message signée avec une clé privée
  Pour le contrôle d'intégrité, d'origine et de non-répudiation des données

  - RSA, DSA

Recommandations : Longueur des clés

- La sécurité des algorithmes repose sur :
  - Leur robustesse face aux attaques (conception)
  - La puissance de calcul disponible
  - Les avancées de la recherche en cryptanalyse

- Allonger la longueur des clés utilisées pour garantir une meilleure sécurité dans le temps.

  La longueur dépendra du problème à résoudre pour qui cherche à décrypter sans la clé.
  - Clés secrètes : recherche des combinaisons possibles
  - Clés RSA : recherche de factorisation de nombres premiers

Recommandations : Longueur des clés

- Des organismes proposant des recommandations
  - Network of Excellence in Cryptology
    http://www.ecrypt.eu.org/
  - National Institute of Standards and Technology
    http://csrc.nist.gov/CryptoToolkit/tkkeymgmt.htmll
  - Bell Labs - Arjen K. Lenstra
    http://cm.bell-labs.com/who/akl/index.html

Recommandations - synthèse

	Algorithmes symétriques (AES)	Algorithmes asymétriques (RSA)	Algorithmes de hachage (SHA)
Années 2006-2010	80 bits	1024 bits	160 bits
Années 2011-2020	100 bits	2048 bits	224 bits
Années 2021 et plus	120 bits (et plus...)	+3000 bits	256 bits

Bibliographie

- Cryptographie appliquée
  de Bruce Schneier - Editions Vuibert
- Histoire des codes secrets
  de Simon Singh - Livre de poche
- Crypto FAQ sur le site RSA Laboratories
  http://www.rsasecurity.com/rsalabs/node.asp?id=2152
- ECRYPT Yearly report on algorithms and keysizes
  http://www.ecrypt.eu.org/documents/D.SPA.10-1.1.pdf
- Cryptographic Key Length Recommendation
  http://www.keylength.com/
- Google
  http://www.google.fr/search?q=cryptographie